Anomaly Detection in ICS Datasets with Machine Learning Algorithms

By: Mubarak, S (Mubarak, Sinil)[1]; Habaebi, MH (Habaebi, Mohamed Hadi)[1]; Islam, MR (Islam, Md Rafiqul)[1]; Rahman, FDA (Rahman, Farah Diyana Abdul); Tahir, M (Tahir, Mohammad)[2]

COMPUTER SYSTEMS SCIENCE AND ENGINEERING
Volume: 37 **Issue:** 1 **Pages:** 33-46
DOI: 10.32604/csse.2021.014384
Published: JUL 2021
Document Type: Article
View Journal Impact

Abstract

An Intrusion Detection System (IDS) provides a front-line defense mechanism for the Industrial Control System (ICS) dedicated to keeping the process operations running continuously for 24 hours in a day and 7 days in a week. A well-known ICS is the Supervisory Control and Data Acquisition (SCADA) system. It supervises the physical process from sensor data and performs remote monitoring control and diagnostic functions in critical infrastructures. The ICS cyber threats are growing at an alarming rate on industrial automation applications. Detection techniques with machine learning algorithms on public datasets, suitable for intrusion detection of cyber-attacks in SCADA systems, as the first line of defense, have been detailed. The machine learning algorithms have been performed with labeled output for prediction classification. The activity traffic between ICS components is analyzed and packet inspection of the dataset is performed for the ICS network. The features of flow-based network traffic are extracted for behavior analysis with port-wise profiling based on the data baseline, and anomaly detection classification and prediction using machine learning algorithms are performed.

Keywords

Author Keywords: Industrial control system; SCADA; intrusion detection system; machine learning; anomaly detection

Author Information

Reprint Address:
International Islamic University Malaysia Int Islamic Univ Malaysia, Jalan Gombak, Kuala Lumpur 53100, Selangor, Malaysia.
Corresponding Address: Habaebi, MH (corresponding author)

− Int Islamic Univ Malaysia, Jalan Gombak, Kuala Lumpur 53100, Selangor, Malaysia.
Organization-Enhanced Name(s)
International Islamic University Malaysia

Addresses:

− [1] Int Islamic Univ Malaysia, Jalan Gombak, Kuala Lumpur 53100, Selangor, Malaysia
Organization-Enhanced Name(s)
International Islamic University Malaysia

+ [2] Sunway Univ, Subang Jaya 47500, Selangor, Malaysia

E-mail Addresses: habaebi@iium.edu.my

Funding

Funding Agency	Grant Number
Publication-Research initiative grant scheme	P-RIGS18-003-0003

View funding text

Publisher

TECH SCIENCE PRESS, 871 CORONADO CENTER DR, SUTE 200, HENDERSON, NV 89052 USA

Journal Information

Impact Factor: Journal Citation Reports

Categories / Classification

Research Areas: Computer Science

Web of Science Categories: Computer Science, Hardware & Architecture; Computer Science, Theory & Methods

See more data fields

Cited References: 20

Showing 20 of 20 **View All in Cited References page** *(from Web of Science Core Collection)*

1. **An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems** — Times Cited: 50
By: Almalawi, Abdulmohsen; Yu, Xinghuo; Tari, Zahir; et al.
COMPUTERS & SECURITY Volume: 46 Pages: 94-110 Published: OCT 2014

2. **SCADA networks anomaly-based intrusion detection system** — Times Cited: 3
By: Almehmadi, A.
P IEEE IND APPL SOC Pages: 1-4 Published: 2018

3. **Time is of the Essence: Machine Learning-based Intrusion Detection in Industrial Time Series Data** — Times Cited: 17
By: Anton, Simon Duque; Ahrens, Lia; Fraunholz, Daniel; et al.
2018 18TH IEEE INTERNATIONAL CONFERENCE ON DATA MINING WORKSHOPS (ICDMW) Book Series: International Conference on Data Mining Workshops Pages: 1-6 Published: 2018

4. **Employing a machine learning approach to detect combined internet of things attacks against two objective functions using a novel dataset** — Times Cited: 1
By: Foley, J.; Moradpoor, N.; Ochen, H.
Security and Communication Networks Volume: 2020 Issue: 2 Pages: 1-17 Published: 2020

5. Title: [not available] — Times Cited: 1
Group Author(s): ISA
Security for industrial automation and control systems, Part 3-3: System Security Requirements and Security Levels Published: 2013

6. **Privacy Preservation Intrusion Detection Technique for SCADA Systems** — Times Cited: 7
By: Keshk, Marwa; Moustafa, Nour; Sitnikova, Elena; et al.
2017 MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS CONFERENCE (MILCIS) Book Series: Military Communications and Information Systems Conference Published: 2017

7. **Intrusion detection in SCADA systems using machine learning techniques** — Times Cited: 1
By: Maglaras, L. A.; Jiang, J.
THESIS Published: 2018
Ph.D. Thesis
Publisher: University of Huddersfield, UK

8. **An Empirical Evaluation of Deep Learning for Network Anomaly Detection** — Times Cited: 5
By: Malaiya, Ritesh K.; Kwon, Donghwoon; Suh, Sang C.; et al.
IEEE ACCESS Volume: 7 Pages: 140806-140817 Published: 2019

9. Title: [not available] — Times Cited: 1
By: McMillen, D.
Security attacks on industrial control systems Published: 2016
Online Available
URL: https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

10. **Machine learning for reliable network attack detection in scada systems** — Times Cited: 1
By: Perez, R. L.; Adamsky, F.; Ridha, S.; et al.
17 IEEE INT C TRUST Published: 2018
[Show additional data]

11. **Machine learning for cybersecurity 101** — Times Cited: 1
By: Polyakov, A.
Dzone, AI Zone Published: 2018
Online Available
URL: https://dzone.com/articles/machine-learning-for-cybersecurity-101

12. **An Anomaly Detection Technique for Deception Attacks in Industrial Control Systems** — Times Cited: 1
By: Qassim, Q. S.; Ahmad, A. R.; Ismail, R.; et al.
2019 IEEE 5TH INTL CONFERENCE ON BIG DATA SECURITY ON CLOUD (BIGDATASECURITY) / IEEE INTL CONFERENCE ON HIGH PERFORMANCE AND SMART COMPUTING (HPSC) / IEEE INTL CONFERENCE ON INTELLIGENT DATA AND SECURITY (IDS) Pages: 267-272 Published: 2019